

## ELECTRONIC MAIL SERVICE MANAGER WITH AUTHENTICATING FUNCTION

Patent Number: JP10133972  
Publication date: 1998-05-22  
Inventor(s): HASEGAWA AKIRA  
Applicant(s): NEC CORP  
Requested Patent: ☐ JP10133972  
Application Number: JP19960305791 19961031  
Priority Number(s):  
IPC Classification: G06F13/00  
EC Classification:  
Equivalents:

---

### Abstract

---

**PROBLEM TO BE SOLVED:** To provide an electronic mail service enabling authentication with respect to a user accessing to a transferring file by means of an electronic mail server by reducing the traffic of a network.  
**SOLUTION:** An electronic mail client 1 transmits an electronic mail text added with a file transferring script including positional information of a file and the name of the file to an electronic mail server 7. The server 7 stores the transferred file in a file server 12 and authenticates the permission of access with respect to an electronic mail client 1' requesting reception to the transferred file based on the file transferring script and mail header information, and only a user who is permitted to access transfers the file from the server 12.

---

Data supplied from the esp@cenet database - I2

要 求 項 の 数 4		要 求 項 の 数 4
(51) 出願番号	特願平 8-305791	(71) 出願人
(52) 出願日	平成 8 年 (1996) 10 月 31 日	(72) 発明者
		(74) 代理人

(54) 発明の名称 認証機能を持つ電子メールサーバ・システム

(57) 要約

【課題】 ネットワークのトラフィックの軽減を可能とし、電子メールサーバで転送ファイルに対してアクセスするユーザに対する認証を可能とした電子メールサーバ・システムを提供。

【解決手段】 電子メールクライアント 1 が電子メール本文にファイルの位置情報及びファイル名を含むファイル転送スクリプトを電子メール本文に付加して電子メールサーバ 7 に送信し、電子メールサーバ 7 はファイルサーバ 12 に転送ファイルを送信し、転送ファイルに対して、受信要求を行った電子メールクライアント 1' に対して、アクセスの許可を認証を行い、アクセスが許可されたユーザのみがファイルサーバ 12 からファイル転送を行うことができるように構成される。

(2) 特開平 10-133972

サーバにファイル転送を行い、受信側のオペレータは、ファイルサーバに転送されているファイルを、自動的にダウンロードを行う、というものである。

【0004】 第 2 の方法は、送信側の端末でバイナリデータをテキスト形式にエンコードしたファイルをメール本文に添付して電子メールを、送信先のユーザ宛てに電子メールサーバに送信する、というものである。この場合、受信側のオペレータは、受信した電子メールから、元のバイナリデータへ復元するためのテキスト形式からのデコードを行う。

【0005】

【発明が解決しようとする課題】 イントラネット化されたネットワーク環境であれば、上記した第 1 の方法によるファイル転送が可能であるが、通常、ファイルサーバに転送したファイルに対してアクセスを制限する機能をクライアント側から設定することはできない。このため、ファイルサーバにログイン可能なクライアントのユーザであれば、誰でも当該ファイルにアクセスすることができ、ファイルのデータの機密性が保たれない、という問題点を有している。

【0006】 一方、上記した第 2 の方法は、電子メールの本文にバイナリデータをエンコードしてテキスト化したファイルを添付することにより、バイナリデータやアプリケーションプログラムを電子メールにて転送するものであるが、電子メールのファイルサイズが増大するという問題点を有している。

【0007】 すなわち、通常、バイナリデータをテキスト形式にエンコードする際、エンコードするソフトウェアにもよるが、元のバイナリファイルのサイズに比べて、テキスト形式に変換されたファイルはそのサイズが 35〜40% も増加する。例えば 10 Kbyte の程度のファイルであれば、それと問題ではないが、数百 Kbyte、数 Mbyte を越えるアプリケーションプログラムやバイナリデータを送信する場合に必要となると、電子メールサーバやネットワーク自身にも多大な負荷を与える、ことになる。

【0008】 したがって、本発明は、上記問題点に鑑みてなされたものであって、その目的は、電子メールサーバにファイルサーバ管理機能を提供し、通常、電子メールの本文に添付され送信されているバイナリデータを、電子メール本体とは別にファイル転送処理する機能を電子メールツールと電子メールサーバ・システム・サーバに有することにより、バイナリデータの添付された電子メールの送信に生じているネットワークのトラフィックの軽減を可能とし、さらに電子メールサーバで転送ファイルに対してアクセスするユーザに対して認証を行うことを可能とした、電子メールサーバ・システムを提供することにある。

【0009】

【課題を解決するための手段】 前記目的を達成するた

め、本発明による認証機能を持つ電子メールサーバシステムは、通信ネットワークシステムを利用している電子メールクライアントが電子メールのメッセージテキスト内にファイル転送指定のコンマドスク립トを挿入して電子メールサーバに送信し、前記電子メールサーバ側において、通常の電子メールの送信/受信とは別に、前記電子メールクライアントからの前記ファイル送信指定コンマドスク립トを受付けて処理を行い、電子メールクライアントからのファイル受信要求に対しては、アクセスするユーザの認証の処理を行う、ことを特徴とするものである。

【0010】

【発明の実施の形態】 本発明の実施の形態について図面を参照して以下に説明する。図1は、本発明の実施の形態の構成を示す図である。本発明は、その好ましい実施の形態において、電子メールクライアント1から送附された電子メールに添付されたファイル転送スク립トに従い、電子メールサーバ7は、ファイルの転送要求（送信、受信）を実行する。

【0011】 また電子メールクライアント1からファイルサーバ12に転送されたファイルに対する、送信要求がある場合には、これに対するアクセス権を確認するたため、そのファイルが送附された時の電子メールのヘッダ情報に基づきユーザの認証処理を行う。

【0012】 電子メールクライアントにおいてファイル転送を行う電子メールサーバ7では、ファイル転送スク립ト文を含む電子メールを送信/受信した後、指定ファイルの転送を電子メールサーバ7に要求する。

【0013】 これにより、電子メール本文には、エンコードされたバイナリデータを添付する必要がなくなり、電子メール本文のファイルサイズ自体は小さくなるため、電子メールの送信時に伴うネットワークトラフィックを軽減する。

【0014】 また電子メールサーバ7側では、電子メールサーバからの転送されたファイルは、通常の電子メールのスプーンする領域とは別に、ファイルサーバ12として個別に管理を行うことで、多数のバイナリメールによる通信トラフィックやディスク容量負荷に対する問題を軽減している。

【0015】 さらに本発明の実施の形態においては、転送されたファイルへのアクセス許可を電子メールヘッダ情報を用いることで、任意のユーザがファイルにアクセスすることを防ぐことが可能としている。

【0016】

【実施例】 上記した本発明の実施の形態について更に詳細に説明すべく、本発明の実施例について図面を参照して説明する。

【0017】 図2は、本発明の実施例に係る認証機能を実現した電子メールサーバ7と電子メールサーバ12の構成を示す図である。図2を参照して、認証機

50

能を備えた電子メールシステムは、電子メールクライアント1と、電子メールサーバ7と、から構成される。【0018】 電子メールクライアント1において、オペレータが使用する電子メールサーバ2は、作成した電子メール本文を送信する送信処理部3と、ファイル転送を実行する際に電子メールに添付したファイル転送スク립トの処理を行うファイル転送スク립ト処理部5と、電子メールサーバ7と、電子メールサーバ7とのファイル転送処理部6と、電子メールサーバ7とのファイルアクセス時に必要な認証情報を転送処理する電子メール認証処理部4と、を備えて構成される。

【0019】 電子メールサーバ7は、電子メールサーバ2と、ファイルサーバ12の磁気ディスク1と、から構成されている。電子メールサーバ2は、電子メールクライアント1からの電子メールの受信/送信を行う電子メール処理部10と、ファイル転送処理部11と、を備えて構成されており、電子メール処理部10は、電子メールに添付されたファイル転送スク립トを読み取る転送スク립ト処理部13と、転送ファイルにアクセスするクライアントの認証を確認する認証処理部9と、を備えて構成される。

【0020】 本実施例において、電子メールクライアント1から転送されたデータファイルは、通常の電子メールとは別に、ファイルサーバの磁気ディスク12に保管され、認証処理部9によって認証されたクライアントに対してのみ、ファイル転送処理部11によってアクセスが行われる。

【0021】 本発明の実施例について更に詳細に説明する。

【0022】 まず、電子メールクライアントにおいて、ファイル送信を行う場合について、図3を参照して説明する。

【0023】 通常の電子メールのメッセージは、電子メール作成機能部でテキスト文で作成するが、あるファイル（アプリケーションプログラムやバイナリデータファイル等）を送信する必要がある場合には、そのファイル転送スク립ト文を添付する必要がある。

【0024】 ファイル転送コマンドスクリプトは、図3に示すように、3つの基本部分から構成される。

【0025】 <ファイルの存在位置>：クライアントのオペレータがファイルアクセス許可されているファイルの位置、すなわちクライアントマシン上のディスクもしくはネットワーク上で共有しているディスク上のファイルの位置を示す。なお、この情報は、電子メールの転送先の相手には隠されているものである。

【0026】 <ファイル名>：上記位置に存在するファイル名を示す。またファイル形式は、テキスト形式、バイナリ形式、圧縮形式のいずれの形式であっても問題はない。

【0027】 <転送先のファイルの位置>：転送相手の

性し、そのユーザにのみファイルアクセス許可を発行する。

【0033】 この結果、ユーザは、電子メール中のファイル転送スク립トからファイル名及びその位置を知ることができ、ファイルにアクセスすることが可能になる。

【0034】

【発明の効果】 以上説明したように、本発明は下記記載の効果を実現する。

【0035】 (1) 本発明の第1の実施例は、ネットワークトラフィックとメールサーバの負荷の軽減等という、ことである。

【0036】 その理由は、本発明においては、従来の方式のように電子メール本文にはエンコードされたバイナリデータは添付して伝送することせず、電子メールとは別にファイル転送を行うようにしたためである。このため、本発明によれば、電子メールのファイルサイズ自体は小さくなり、電子メール送信時に伴うトラフィック量は軽減する。

【0037】 (2) 本発明の第2の実施例は、電子メールサーバに転送されたファイルについて、電子メールのヘッダ情報を用いることで、電子メールサーバ側でアクセスの認証を行うことが可能とされ、認証されたユーザのみアクセスが許可されるため、ファイルデータの漏洩性が保たれ、安全性、信頼性を向上するというのである。

【図面の簡単な説明】

【図1】 本発明の実施の形態に係る認証機能付き電子メールシステムを示す図である。

【図2】 本発明の実施例の構成を示す図である。

【図3】 本発明の実施例を説明するための模式図である。

【図4】 本発明の実施例を説明するための模式図である。

【符号の説明】

- 1 電子メールクライアント
- 2 電子メールサーバ
- 3 電子メール送信部
- 4 電子メール認証処理部
- 5 転送スク립ト処理部
- 6 ファイル転送処理部
- 7 電子メールサーバ
- 9 認証処理部
- 10 電子メール処理部
- 11 ファイル転送処理部
- 12 磁気ディスク（ファイルサーバ）
- 13 転送スク립ト処理部

20

電子メールサーバ（ファイルサーバ）名と、その転送ファイルが保存される位置を示す。ただし、この位置情報は、電子メールの転送相手に送って、その電子メールサーバが保存することから、相手側の電子メールを指定した際に、自動的に、保存する電子メールサーバの情報が取得できるものとす。また、電子メールサーバとは、そのサーバ端が存在するネットワークで規定されている一意な記述とする。たとえばIPアドレスもしくはドメイン名付与ホスト名で表現する。またファイルの保存する位置とは、ファイルサーバのディスクに置かれたファイルの位置（ディレクトリ階層の位置での情報）を示す。

【0028】 このように生成されたファイル転送スク립トを電子メールの本文に添付し、通常の電子メールと同様に電子メールサーバ7に転送される。

【0029】 なお、このファイル転送スク립ト文は、電子メールのメッセージ文中であれば、何処に挿入されていてもよい。またスク립ト文の記述方式としては、オペレータ自身がキーボードからスク립ト文を直接入力するか、又は、電子メールツールでスク립ト文の入力オプションにてネットワーク端末もしくはクライアント端末自身のディスクにあるファイルを選択することができれば、「ファイル」を参照すること、自動的に電子メールのメッセージ文にコマンドスク립ト文が上記のフォーマットで添付される。こうして手動又は自動で作成されたファイル転送スク립ト文を含む電子メールは、上記したように、通常の電子メールと同様に電子メールサーバ7に転送する。

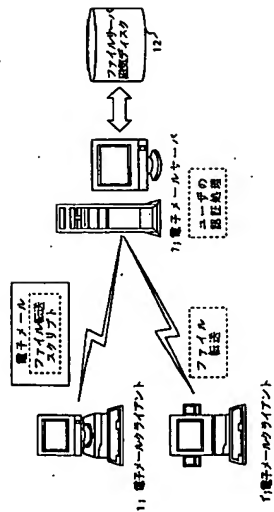
【0030】 次に電子メールサーバ7において、ファイル送信・受信を行う場合について、図4を参照して説明する。

【0031】 電子メールサーバ7において、ファイル転送スク립ト添付された電子メールを受信すると、ファイル転送スク립トで指定されたサーバ名、ファイルの位置情報を確認する。また、その際、その電子メールのヘッダ情報とその転送ファイルと同時に記録する。この電子メールヘッダ情報には、「送信者」と、「メールの送信先ユーザ名」が記述されており、この情報は、後に、このメールの送信先のユーザがファイルにアクセスする際の認証（ユーザ認証）に必要となる。

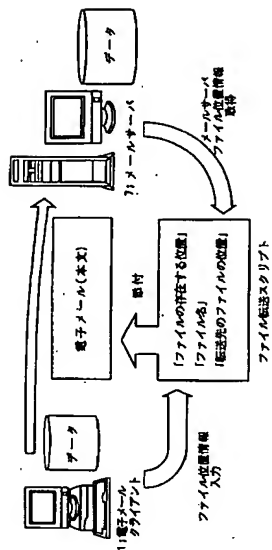
【0032】 電子メールの送信先のユーザ（電子メールクライアント1）が、電子メールサーバ7に対してメールの受信要求を出す、電子メールサーバ7は、上記した電子メールヘッダ情報の宛先ユーザ情報と、アクセス中（受信側電子メールクライアント1）のユーザ情報と、を確認し、正しい場合には、ファイル転送スク립トを添付した電子メールを当該クライアント1に送

30

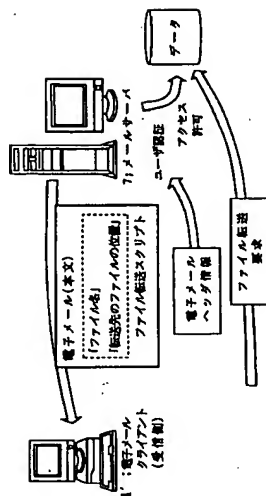
【図1】



【図3】



【図4】



【図2】

